

Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

POLICY

1. General Policy

The City recognizes the use of e-mail and computers by City employees has increased tremendously, raising numerous policy issues with respect to communication, creation of information and systems, retrieval and storage of records, and proper etiquette.

It is the general policy of the City of San José that use of City computer equipment, electronic facilities and electronic data are limited to *official City purposes* only. In general, employees should use the information systems for the City of San José business only. The e-mail system may not be used to solicit or persuade others for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

Electronic mail and information systems of the City are not to be used in a way that may be disruptive, offensive to others, or harmful to morale. For example, the City prohibits the display or transmission of sexually explicit images, messages, or cartoons or any transmission or use of e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability religious or political beliefs.

Technology in the computer and e-mail industry changes rapidly and references to named suppliers in this policy are subject to change without prior notice and modification to the policy. It is understood this policy will continue in full force and effect even if there are future additions and/or deletions to the named suppliers in this policy, if those suppliers are providing the same or similar services.

The following policies apply to the use of e-mail, internet services and other electronic media by City employees:

2. Public Records

- A. All permanent City records, including paper and computerized, are governed by the mandatory public disclosure requirements of the Public Records Act and its exceptions. If a draft record is retained it may become a public record, unless subject to an exception under the Public Records Act.
- B. Electronic mail is not intended for permanent storage. Electronic mail in-trays and out-trays shall be purged on a minimum 90-day basis by the City's Information Technology Department, and, upon implementation of the appropriate technology, the City may, in its discretion, purge any such mail on an automatic basis.

**Use of E-Mail, Internet Services,
and Other Electronic Media****1.7.1**

- C. If the City is required to maintain any electronic mail as a permanent record, it must be printed out in hard copy for permanent filing, or an electronic file shall be copied, archived and stored separately from ordinary in-trays or message logs.
- D. Electronic mail is not backed-up on a permanent basis. The City stores electronic mail only to the degree that allows the City to restore current electronic mail in the event of a systems failure.
- E. Public Records Act Requests should be handled in accordance with standard departmental policy and direction.
- F. The City reserves the right for any reason to access and disclose all messages and other electronic data sent over its electronic mail system or stored in its files.
- G. The City has the right to delete or retain any or all electronic files including e-mail of a City employee who is no longer employed by the City.

3. Attorney-Client Privileged Communications

Some messages sent, received or stored on the City e-mail system will constitute confidential, privileged communications between the City and its attorneys. Attorney-client communications should not be forwarded without consulting the City Manager's Office and/or the City Attorney's Office.

4. Confidential Information

Most communication among City employees is not considered confidential. However, certain communications, such as police investigations and personnel records, may be confidential or contain confidential information. Questions about whether communications are confidential should be raised with the employee's supervisor.

- A. Employees shall exercise caution in sending confidential information on the e-mail system as compared to written memoranda, letters or phone calls, because of the ease with which such information may be retransmitted.
- B. Confidential information should not be sent or forwarded to individuals or entities not authorized to receive that information and should not be sent or forwarded to other City employees not directly involved with the specific matter.

Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

- C. Care should be taken in using e-mail to ensure messages are not inadvertently sent to the wrong individual. In particular, exercise care when using distribution lists to make sure all addressees are appropriate recipients of the information. Lists are not always current and individuals using lists should take measures to ensure lists are current.
- D. Employees shall not discuss confidential information outside of the workplace.
- E. Confidential information should not be reproduced unnecessarily.
- F. Employees shall return all tangible forms of confidential information to the City upon termination of employment or at the City's request.

5. Internet and Intranet Services

The City of San José has internet access to the Information Superhighway through a local service provider. The City also provides an intranet server.

The Internet project provides direct access over high-speed data lines for the following services:

- E-mail
- News group discussions
- FTP file transfers
- Telnet sessions
- Gopher services
- Web services
- City of San José Web page for external Internet users to receive a wide range of public information about the City of San José.

The Intranet project provides direct access on the City network and provides for the following services:

- Information postings
- Policies and procedures
- Employment opportunities
- Discussion groups
- Newsletters and bulletins

The following policies are applicable to these services:

- A. All access for Internet and Intranet must be approved by Department Directors.

**Use of E-Mail, Internet Services,
and Other Electronic Media****1.7.1**

- B. Employees shall not create new discussion groups on Internet or Intranet without departmental approval.
- C. Departments shall designate a 'Content Manager' for point of contact with ITD and the City Manager's Office.
- D. The City will provide training for City employees in both Internet and Intranet services. City employees should receive training before using these services.
- E. City departments shall use the City's Internet home page for all Internet postings and Intranet home page for Intranet postings, and shall not initiate new or separate services outside of the City's designated services without the consent of ITD or the City Manager's Office. Internet and Intranet home pages external to the City's official sites must be linked to these home pages.
- F. City departments shall post information to the Intranet and Internet using guidelines provided by ITD.
- G. The decision of the City Manager's Office for appropriateness of materials and usage of Internet and Intranet services shall be final.
- H. Department Directors have primary responsibility to ensure adherence to this policy.
- I. ITD has technical responsibility for setting up and managing Internet and Intranet resources, including user account maintenance.
- J. The following policies are applicable to downloaded information:
 - 1. Information downloaded from the Internet or Intranet shall be for City work related purposes only.
 - 2. Downloaded information including e-mail attachments shall be checked for virus contamination. Each department has information available on how to make this check.
 - 3. Downloading of large data images, video and graphics should be timed so as not to impact the performance of the City network. Very large files should be downloaded after normal working hours.
- K. Internet broadcast services must be approved by the Department Director, or designee. Internet broadcast services must utilize the centralized ITD broadcast servers when available.

Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

6. Intellectual Property Rights

- A. It is the City of San José's policy to retain all copyrights and other intellectual property rights of which it is the legal owner. All copyrights and other intellectual property rights which are created by City employees in the course and scope of their employment by the City of San José are the exclusive property of the City of San José.

EXCEPTION: Works created under the following circumstances are excluded from this policy:

1. Works developed entirely by the employee on the employee's own time without using City equipment, supplies, facilities, or trade secret information except for those creations that either:
 - (a) Relate at the time of conception or production to the City's business, or actual or demonstrably anticipated research or development of the City; or
 - (b) Result from any work performed by the employee for the City.

For example, an employee may retain rights to artwork, photographs, writings which are created by the employee at home, which are not related to the employees' work and not intended to be used or purchased by the City of San José.

2. Copyrights or other intellectual property rights which are created pursuant to an authorized written agreement between the City of San José and the employee which gives a property right to the employee. Agreements shall not be authorized without prior written approval of the City Manager, or designee.

B. Transfer of Information

1. City employees shall not post material on Internet or Intranet services or send material via e-mail which is copyrighted by a party other than the City.
2. City employees shall not download copyrighted materials from these services.
3. Employees shall not transfer or use in the performance of their duties any proprietary or confidential information, whether or not in writing, of a former employer without that employer's written consent.

Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

7. Security

- A. City of San José information technology systems shall be protected from intrusion from outside sources, as follows:
 - 1. The City shall construct fire walls to prevent outside sources from using telnet and File Transfer Protocol (ftp) to gain access to the City system except where authorized by ITD.
 - 2. Inbound Internet services shall be limited to e-mail (SMTP), and newsgroups (NNTP).
 - 3. The public shall not have direct access to the City's Intranet server. All public access will be through the Internet server.
- B. The City reserves the right for any reason to access, disclose and delete all messages and other electronic data sent over its electronic mail system or stored in its files.

8. Employee Responsibilities

- A. Employees shall not enter or attempt to enter computer files and communications of another individual without the employee's authorization or consent, or the consent of the City Manager's Office.
- B. Suspected or identified security violations shall be reported to ITD. Violators may lose Internet access and may be subject to disciplinary action.
- C. Employees shall not use re-mailing services, or use "anonymous" or "aliases" to protect their individual identities while using City information technology systems or equipment.
- D. Employees should regularly change their individual passwords. Employees shall not share individual passwords with other individuals except for legitimate City business reasons.
- E. Employees shall not use, or attempt to use, another employee's password without the employee's consent.
- F. All communications should follow proper etiquette, such as:
 - 1. Materials posted by City employees shall professionally represent the City of San José. The transmission of defamatory, obscene, offensive or harassing messages,

**Use of E-Mail, Internet Services,
and Other Electronic Media****1.7.1**

or messages which disclose personal information without authorization is prohibited.

2. E-mail messages and electronic postings may be read by people beyond the addressee, and upon request may be produced to a court in connection with litigation and should be composed accordingly.
- G. Employees shall not send mass electronic mail messages on a “City-wide” basis to all employees without prior written authorization of the Department Director, or designee.
- H. Employees should carefully consider the names on a mailing list as addressees or copies. Some employees may not want their e-mail addresses to be widely known or to receive responses to widely distributed messages.
- I. Misaddressed e-mail shall be sent back to the original sender with a message that the message has been misaddressed, and the original deleted. However, if the misaddressed electronic mail is offensive, inappropriate or otherwise in violation of this policy, the misaddressed e-mail shall be forwarded to the recipient’s Department Director or designee for appropriate action.

Approved:

/s/ Debra J. Figone

Approved

8/15/97

Date